NAVAL WAR COLLEGE
Newport, R.I.

THE PEOPLE SIDE OF INFORMATION WARFARE

by

James H. Weidner

Lieutenant Colonel, United States Air Force

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: James H. Weidner

14 June 1995

Paper Directed By Captain D. Watson
Chairman, Joint Military Operations Department

UNCLASSIFIED
Security Classification This Page

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification):
THE PEOPLE SIDE OF INFORMATION WARFARE (U)

9. Personal Authors:
JAMES H. WEIDNER, LIEUTENANT COLONEL, UNITED STATES AIR FORCE

10. Type of Report: FINAL

11. Date of Report: 16 JUNE 1996

12. Page Count: [redacted] 31

13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: INFORMATION WARFARE, INFORMATION WARRIORS, INFORMATION AGE WARFARE, EXPERT SYSTEMS, ARTIFICIAL INTELLIGENCE, COMMAND AND CONTROL WARFARE, C4I FOR THE WARRIOR, INFOSPHERE, INTELLIGENCE, INFORMATION, CYBERSPACE

15. Abstract: Whether at the strategic, operational or tactical level of war, success has become directly related to getting the right information to the right person at the right time. Information-based technologies have permitted orders-of-magnitude increases in the speed at which information can be transmitted, processed, and accessed. Always a concern when dealing with such potentially large quantities of real-time information is the problem of information overload of the users. What will be the impact of this information flow on the individuals at the human-machine interface? Recently, a few notable authors have expressed reservations about the promises of information warfare. Interestingly, those reservations center on issues related to getting enough talented people to serve as information warriors. This paper examines some of the issues related to the people side of information warfare. Arguably, the real center of gravity is not information but rather the information warriors themselves. The challenge will be, as it has always been, to ensure that we have enough talented individuals to get the job done.

16. Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**

17. Abstract Security Classification: UNCLASSIFIED

18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. Telephone: 841-[redacted]6461

20. Office Symbol: C

Security Classification of This Page Unclassified

Abstract of

THE PEOPLE SIDE OF INFORMATION WARFARE

Whether at the strategic, operational or tactical level of war, success has become directly related to getting the right information to the right person at the right time. Information-based technologies have permitted orders-of-magnitude increases in the speed at which information can be transmitted, processed, and accessed. In conjunction with the rapid production and exchange of information, large databases continue to be generated as the amounts of required and useful information have mushroomed.

Always a concern when dealing with such potentially large quantities of real-time information is the problem of information overload of the users. What will be the impact of this information flow on the individuals at the human-machine interface? Will additional education and specialized training be needed for users? Does more dependence on artificial intelligence (AI) become necessary?

Recently, a few notable authors have expressed reservations about the promises of information warfare. Interestingly, those reservations center on issues related to getting enough talented people to serve as information warriors. This paper examines some of the issues related to the people side of information warfare.

Arguably, the real center of gravity is not information but rather the information warriors themselves. People will make the critical difference. They always have. The challenge will be, as it has always been, to ensure that we have enough talented individuals to get the job done.

The People Side of Information Warfare

Whether at the strategic, operational or tactical level of war, success has become directly related to getting the right information to the right person at the right time. The National Military Strategy indicates that winning the information war is one of our basic principles for future use of military force. And, it emphasizes "[t]he leverage attainable from modern reconnaissance, intelligence collection and analysis, and high-speed data processing and transmission warrants special emphasis."[1] Information-based technologies have permitted orders-of-magnitude increases in the speed at which information can be transmitted, processed, and accessed. In conjunction with the rapid production and exchange of information, large databases continue to be generated as the amounts of required and useful information have mushroomed. Indeed, this expanding world of information and associated information systems has become known as the infosphere.[2]

Using the infosphere, it is now possible to create a real-time picture of the battlespace that can be viewed simultaneously by all friendly forces. This is the goal for the Global Command and Control System (GCCS) which will implement the JCS concept of "C4I for the Warrior." GCCS is intended to provide "fused real-time situational awareness knowledge in all of its dimensions."[3] Always a concern when dealing with such potentially large quantities of real-time information is the problem of information overload of the users. What will be the impact of this information flow on the individuals at the human-machine interface? Will additional education and specialized training be needed for users? Does more dependence on artificial intelligence (AI) become necessary?

Some experts believe that information warfare will place even greater demands on information warriors. Recently, a few notable authors have expressed reservations about the promises of information warfare. Interestingly, those reservations center on issues related to getting enough talented people to serve as information warriors. This paper examines some of the issues related to the people side of information warfare. And, as will be seen, the people most directly impacted by the changing nature of war may be the operational commanders.

The Air Force defines both information age warfare and information warfare. The first term refers to the application of "information technology as a tool to impart our combat operations with unprecedented economies of time and force."[4] Information warfare, on the other hand, "views information itself as a separate realm, potent weapon, and lucrative target."[5] This raises some questions regarding who will perform the tasks associated with information age warfare and who will perform the tasks of information warfare. The position taken here is that the same individuals must be able to do both sets of tasks for several reasons. First, there will be considerable overlap between the two given that use of the associated computer network interfaces demands like knowledge and skills. Second, we won't be able to support two separate pools of elite infosphere navigators. Third, it will be extremely difficult to draw a clear line between the two particularly when the defensive side of information warfare is examined. Those who are using the infosphere to support combat operations will have to be intimately familiar with defending the integrity of their information and, therefore, well-informed about the latest tools of offensive information warfare. Last, but not least, it would be most unfortunate if the more talented personnel were placed in a separate group dedicated exclusively to information warfare since that could seriously undermine the ability of combatant commanders to conduct conventional operations or information age warfare. This last point merits some additional consideration.

Advocates of information warfare appear to be guilty of the classic 'mirror imaging' in trying to envision a future adversary. It is not clear how any peer competitor will emerge in the forseeable future to challenge our complete dominance of the infosphere. That would mean defensive measures are certainly warranted to defend our information systems, but that the extraordinary means of conducting offensive information warfare (viruses, surreptitious alteration of databases, etc.) are probably better left to the appropriate agencies such as the CIA and NSA. And, as will be seen, to find enough talented people to become information warriors will be a significant challenge for the military. In fact, we need to put a high priority on just keeping up with the real-time tasks now associated with information age warfare.

Information Flow and Staying Afloat

Shortly after a United States F-16 was shot down over Bosnia, the Secretary of Defense observed that "In this case we're talking not about hours or minutes. It's getting the information out to them in a matter of seconds."[6] Not only has the speed at which information can be transmitted dramatically increased, but the amount of all sorts of information readily available to military users has grown to staggering proportions in the pursuit of the goal of achieving dominant battlespace awareness. Concerning information flow, Joint Pub 6-0 notes that it "must be nearly instantaneous vertically and horizontally within the organizational structure" and decision makers "must be able to immediately pull the information they need."[7] This brings up a number of concerns when considering that it's people who will have to act on this real-time information. Based on current trends, commanders at all levels will have precious little time to make critical choices as the observe, orient, decide and act (OODA) cycles are compressed into ever smaller time frames. A report published by the Center for Naval Analyses notes

> Where strategists once spoke of the importance of accurate and timely communications for coordinated battle plans, they now assume that basic communications capability and are concerned instead about executing operations within the opponent's decision cycle--the time it takes the enemy to respond to stimuli and make a decision to react. This evolution is a direct consequence of the technological explosion in the enabling technologies that quickly and accurately convey information--data, pictures, ideas--to diverse components.[8]

Information warfare (IW) goes beyond the traditional bounds of command and control warfare (C2W) in that it includes the possibility of attacking information systems that are not part of command and control. It will change the way the services organize, train, equip and employ forces. The operator at the human-machine interface (HMI) will have access to a virtual flood of real-time information as well as databases of potentially immense size. The requirement for real-time performance is even more critical in IW. Information warriors could be required to make decisions in milliseconds instead of seconds. What automation will be needed to support IW tasks and to what extent will the information warrior maintain control over 'thinking' machines.

Humans in the Loop

For decades, critics of the trend to rely more and more on computers have predicted HMI information overload. A popular text on automatic pattern recognition written in the early 1970s notes

> In recent years our very complex and technologically oriented society has created a situation in which more people and organizations have become concerned with handling information. . . . The need for improved information systems has become more conspicuous, since information is an essential element in decision making, and the world is generating increasing amounts of information in various forms with different degrees of complexity.[9]

What one discovers in reviewing the literature on computers and high-speed communications systems is that for every dramatic increase in the information flow there has been renewed interest in the field of artificial intelligence (AI). The genesis of expert systems followed closely the development of large command, control, communications and intelligence (C3I) systems for the military. Researchers who were for the most part focused on developing the next generation of computers only gradually became aware of the multitude of HMI problems and, as a result, only highly skilled and trained individuals were expected to be able to actually operate an expert system or decision support system (DSS) that incorporated 'thinking' machines. Large simplified displays or status boards were provided for decision makers who were not trained to operate the DSS and, therefore, not able to manipulate it directly. The consensus amongst most computer scientists in the 1970s was that since "robust AI systems were ten to twenty years away. . . [it would be necessary] to 'wire' talented humans into computer systems to expand the problem-solving capacity. . ."[10] As one researcher belatedly observed, "[this] system does not, alas, terminate at its terminals--users are attached."[11] However, as the information flow continued to increase, questions regarding what should be automated and what should not be automated were inevitable. And, the possible failure of an AI system could have very serious consequences if an automated process produced erroneous information that led military decision makers to select unwarranted or unwise courses of action. To avoid information overload AI systems were necessary, but at some point such an approach might require a completely automated decision process to meet near real-time performance requirements. This is essentially the situation today as we address all the ramifications of the evolution of information age warfare and the additional demands of the more revolutionary information warfare.

For the military the use of AI systems has always raised the question of how much control humans should or could retain over what a C3I system or weapons system was doing. Likewise, information warriors will require special AI tools to scan or surveil an adversary's information systems and make almost instantaneous 'strikes' on databases or software code to ensure minimum risk of detection. Can we afford to keep humans in the decision loop given the time constraints? Human control over such tools could be as critical as the need to have humans in the decision loop when it comes to possible use of the nation's nuclear missiles during the early years of the Cold War.

An Historical Perspective

Until the late 1970s, the military provided the impetus for research and development (R&D) efforts seeking increased computer processing power and higher throughput for communications systems. In particular, it was the age of nuclear confrontation coupled with the uncertainties of cold-war politics that produced unprecedented performance demands for each new generation of computers and the communications networks that linked them to various sensors and command and control centers. It was during this time frame in which the first large command, control, communications and intelligence (C3I) systems were introduced that the first lessons of information warfare were learned--although it would be almost two decades before that term became popularized.

The Missile Attack Warning System (MAWS) at the North American Air Defense (NORAD) Command's underground facility in Cheyenne Mountain near Colorado Springs, Colorado was the heart of the nation's defense against any Soviet nuclear attack. Built in the 1960s, this underground facility was hardened against nuclear effects and made extensive use of survivable communications to connect it to various sensors and other command posts through a C3I system called the National Military Command System (NMCS).[12] Using a "spoke and ring" configuration to avoid single points of failure, the Close-in Automatic Route Restoral System (CARRS) connected the underground facility to the nationwide telephone system. Bell Laboratories designed the special electronic pathfinder that constantly monitored the status of all the communications circuits and restored or rerouted message traffic as required.[13] Certainly, the connection to the telephone system would in today's information warfare environment be considered a potential problem area because hackers might be able to access the MAWS computers and, for example, create a false missile alert. As it turned out, the real problems were internal ones in the form of a technician who accidentally ran a training tape producing false indications of a mass raid on November 9, 1979 and a faulty chip in a communications processor computer which produced similar false indications on June 3 and June 6, 1980.[14] The subsequent Senate investigation into the false alerts produced a report documenting a number of problems with the MAWS and making some important observations about the reliance on computers. That report noted that

> ...the missile tactical warning and threat assessment task is a very complex and difficult technical task....to accomplish it we rely on a combination of satellites and ground-based radars located around the world coupled with computers and communications systems to bring the data together, analyze it and transmit it to those who need it in a very short period. We could not do this task without computers and high-speed communications systems....But even though we are dependent on computers and high-speed communications, we are not controlled by them. At every step of the process, experienced trained personnel evaluate and make judgments on the meaning of the data and only these personnel can direct any action in response to what the warning system tells us.[15]

Note the emphasis on having people in the decision loop. When we consider the tasks of information warfare, it is clear that the complexities involved will be orders of magnitude greater than those associated with the task of missile tactical warning and threat assessment. Clearly we can't accomplish these tasks without an even greater reliance on computers and high-speed communications systems. Also, more reliance on AI systems which can automate many decision processes will greatly increase the need for defensive measures to protect the integrity of our command and control (C2) systems.

The Senate report played down the significance of the false alerts noting that SAC's quick response "was a prudent step to enhance the survivability of the bombers and tankers should this country be under attack."[16] The Soviets, however, were unimpressed with our explanations and rationalizations, and they accused the United States of "playing games that could lead the world to nuclear war."[17] This points out the seriousness of having false data introduced into critical C2 systems whether it is done intentionally from some external source or unintentionally generated within the electronics of the C2 system itself. One can imagine the problems of controlling the 'launching' of viruses into an adversary's C2 system. How will we predict the response? How would 'false alerts' be interpreted by a less cautious enemy?

It didn't take Hollywood long to bring such a scenario to the silver screen. In 1983 the movie Wargames alerted Americans to the potential dangers of home computers connected to the nationwide telephone system. In the movie a high school student manages to access the NORAD computer using his personal computer and begins to play a 'game' which inadvertently ends up taking the world to the brink of thermonuclear disaster. He even manages to alter his grades for the better by cleverly tapping into the school computer. A review in Newsweek noted the movie was "really less an anti-nuke film than an anti-computer movie, in the great 'Frankenstein' tradition of the manmade monster taking control of man."[18] Today, the dangers of hackers are ever present and what in 1983 was moderately entertaining science fiction has become a nightmare in reality. The review of the movie in The Nation noted the scenario was "so ingenious and absorbing that the Pentagon has felt the need to assure us that nothing of the sort is remotely possible with its equipment, a statement the military would be obliged to make, whatever the facts."[19]

Hackers for Hire?

The likelihood of anything like Wargames actually occurring was debatable. Perhaps it was somewhat more plausible when the Federal Bureau of Investigation (FBI) revealed the escapades of Kevin D. Mitnick, a notorious hacker finally apprehended by in February 1995 after almost three years of international flight. Mitnick was interviewed for the first time by a journalist from Computerworld shortly before his capture. The article containing that interview noted "...[he] personifies the hacker as sociopath. His exploits--legend has it he penetrated the North American Air Defense Command as a teenager--are said to have inspired the movie Wargames."[20] Here, then, we get a glimpse of the type of person who becomes a hacker as Mitnick describes how he started perfecting his skills.

> Five years ago, that's all I looked forward to, even in my marriage. I put my hacking above my work, my time with my wife, anything. At the time I knew I had this drive to do it, but I didn't think about it.[21]

It is unlikely that DOD would hire hackers such as Mitnick. However, what sort of training and educational background will it take to produce an information warrior with that kind of talent? And, to maintain the necessary skills for war in Cyberspace will certainly demand constant devotion to the cause. Some pundits are now calling for creation of an information corps that could provide the necessary information warriors for joint operations.

Open-Source Intelligence

Wilson and Bunkers also point to the need to get more information and get it more quickly and in higher quality than our adversaries. They are concerned about the military's ability to obtain and utilize the vast amounts of open-source intelligence (OSInt) now available. Specifically, with respect to the Marine Corps, they see as a solution making Marines "global-information warriors."[22] This, again, raises the issues of education and training. How do we get the educated recruits and what training will permit them to compete with say a Kevin Mitnick? Does the military really need OSInt?

The Information Corps Approach

Libicki and Hazlett argue that creation of a separate organization for information warriors is the only way to ensure that we will be able to take full advantage of the information revolution in the near term. This approach, they argue, would automatically resolve tough issues such as jointness by putting the information corps in something like a special operations command status out of reach of interservice rivalries. They indicate

> The logical conclusion is that DOD should form an Information Corps. The argument is that a corps would promote jointness where it is critically needed (information interoperability), elevate information as an element of war, develop an information warrior ethos and curriculum, and heighten DOD attention to the global civilian net.[23]

But the issues associated with proper education and training of personnel assigned to such an Information Corps present some particularly alarming prospects. Lubicki and Hazlett discuss at length just how complex this might be, and it is easy to see what demands such an expansive career development program will make on time and resources.

> As computers get more sophisticated, training necessary for their effective use may get longer. The information warrior must know not only programming but systems integration and systems theory, communications, security, artificial intelligence, logic in all its

> many forms (classical, fuzzy, and convergent), and statistical techniques. The information warrior must also know the customer's needs: the commander's intent, doctrine, and strategies. In addition, the information warrior should know something about specific media (land, sea, and space). . . .The amount of information necessary to be an information warrior is immense, and the time required to master it will have to be at the expense of more general command instruction.[24]

Based on this proposed education and training, it is safe to say that those joining the Information Corps would be considered elite personnel. What the authors describe as necessary skills for information warriors will be highly marketable skills in the business world. It is difficult to see how there will be enough time and money to support such extensive education and training, let alone keep these very specialized individuals in uniform given the great demands for their talents by almost every major corporation. The alternative is to once again turn to AI systems which can perform many tasks without direct supervision. The tradeoffs are increased research and development (R&D) costs to develop expert systems and the inherent risks in relying on automation or 'thinking machines' to perform some key tasks. The establishment of an Information Corps is clearly not a panacea for all real or perceived problems in carrying out a revolution in military affairs that would foment the desired capabilities in information warfare. A more viable approach may be to better utilize AI systems, and ensure we properly 'wire' talented operational commanders to them so that there is a more seamless interface between those who tap into the information flow and those decision makers who rely on information as the lifeblood of battle management. Recognizing that in the future all military personnel will need to have some of the basic skills required of information warriors, it is the operational commander who stands out as the most important link between operational art and information warfare.

Operational Commanders and the Information Revolution

Given that the degree of success of information warfare will be highly dependent on the very people or information warriors who employ its tools, it is necessary to consider its relationship with operational art to fully appreciate both the potential capabilities and problem areas. Because operational art integrates the key activities of all levels of war, it can be argued that the linkages between information warfare and operational art will be particularly important. Here, then, we must consider the role of the operational commander.

An article in Armor recently pointed to just how much impact the information revolution has had even on tank commanders. The information systems provided with the new M1A2 tank have greatly improved battlefield awareness. However, the Intervehicular Information System (IVIS) could produce an information overload. The author notes that "[for] the M1A2 task force, instead of confusion on the battlefield being caused by absence of information, confusion can be caused by the sheer volume and clutter of data."[25] He indicates that we "need leaders who are capable of managing and interpreting large volumes of information. . . .they must be familiar with computers, the management of files and manipulation of software."[26] Finally, he observes "[t]he days of the computer illiterate armor leader are going the way of the horse cavalry soldier."[27] If the demands at the tactical level are so great, then the demands on operational commanders will certainly be even greater.

Walsh foresees considerable shortening of the decision cycle for tactical ground commanders through information enhancement which increases the quantity and quality of battlefield information as well as the speed at which it is transmitted to users. Noting the long-standing emphasis on strategic reconnaissance and surveillance by the Air Force, he advocates next-generation systems which can support all levels of war. The objective is to provide a common view of the battlefield which provides synergy amongst friendly forces while reducing the risk of fratricide. Walsh indicates that "ground forces would like to deploy larger numbers of relatively low-cost, smaller systems down to the battalion level."[28] The near real-time performance for proper use of such tactical reconnaissance systems and the need to push as well as pull information into and out of the network to which they are connected will demand highly trained operators--the information warriors supporting tactical ground commanders.

An article in the November 1994 issue of Military Review highlighted the need for developing theater information strategies to support unified commanders and ensure that information warfare at the operational level of war could be successfully waged in concert with efforts at the strategic and national-strategic levels. The author proposed an increased focus on theater information strategies as a means of deterring potential enemies and being prepared to conduct appropriate psychological operations (PSYOP) together with necessary public affairs programs should conflict become inevitable. In order to ensure unity of effort, he indicated that "J5s at the unified command level would routinely convene an information coordinating committee to coordinate the various efforts..."[29] Such coordination would ensure that political, economic and military aspects of any information war were properly harmonized on an interagency basis as well as with allied nations. From the joint perspective, the author emphasized

> At the joint staff level, the Joint Strategic Planning System would be modified to ensure this political-military context is not only considered during planning, but is also included as part of both the friendly situation and the commander's intent in all subordinate

> planning documents such as warning orders, operations plans, contingency plans and operation orders.[30]

With respect to the tools required by operational commanders to orchestrate formulation of theater information strategies, the author only reflected on the need to employ technology to make sure the information flow was directed to the right people. The presence of any such tools certainly would demand a permanent team of information warriors somewhere in the unified command structure. This, of course, stands in sharp contract to the proposal to create an entirely separate Information Corps. Clearly, all of the operational commanders will require an organic capability to properly plan for and conduct information warfare.

Boyd and Woodgerd note that the increasing dependence on information flow "will likely change the way we command military operations."[31] Importantly, they address the essential leader development for success stressing that

> ...the complex nature of future operations may require leaders of greater experience and rank commanding at lower levels....[and] all future leaders will be called upon to make rapid, doctrinally sound decisions as they plan and execute missions in more diverse, high-pressure operational environments.[32]

The need to become familiar with navigating the infosphere is obvious. Future operational commanders will have to become well-versed in use of the decision support systems (DSS) that make sense out of the river of information that will flow on modern battlefields and across all theaters of operation. They will have to ensure that there are information warriors to keep the necessary information flowing to the right people at the right time. But the job of decision making rests squarely on the shoulders of the commander.

Madigan and Dodge indicate that commanders must have appropriate cognitive skills to take full advantage of available information. A continuous cycle of assimilation, visualization and conceptualization allows commanders to use the current picture of the battlespace to select courses of action that will meet the immediate objectives and take into account the desired end state. They note that

> The best intelligence and friendly force information are worthless unless the commander knows when to act and is willing to act. No matter how well automated, no matter what level of technological sophistication of the process and procedures built into command and control hardware and software, systems do not make decisions; commanders do.[33]

However, once the information flow is so great as to significantly risk information overload, there is the inevitable tendency to automate at least some part of the decision process or filter out information not considered important to the commander. Both of these could increase the risk of making a a bad decision. And, for information warfare the time frame to make a decision will be compressed to the point that substantial automation may be necessary.

Intelligence and Information

Nowhere is the demand for fast and accurate information greater than in the intelligence community. The collection, processing, and distribution of imagery data, for example, has traditionally pushed the limits of both state-of-the-art computers and high-speed communications systems. And, some of the individuals who have spent many years in that arena are now claiming that the revolution in military affairs is really "nothing more than the military ability to exploit precise intelligence fully" in the use of precision-guided munitions.[34] The problems that arise in doing this are, of course, associated with the transmission of information, or intelligence specifically in this case, on an almost real-time basis and making sure that information is sent to the right person at the right time. Smith argues that

> The real challenges for future intelligence are to limit the uncertainty by acquiring and maintaining the necessary expertise and data bases, to accept the man in the loop as necessary, and to identify how and where in the revolution in military affairs information structure the 'man' can be most helpful.[35]

Smith points to the need to establish "a small core of trained and experienced regional analysts who can integrate diverse intelligence and open-source reporting."[36] And, he advocates the inclusion of intelligence officers at the national level to ensure operational issues are properly addressed in constructing information strategies. So, here again, we see the requirement for specialized individuals to direct the information flow and perform tasks associated with the conduct of information warfare. Interestingly, Smith concludes his article with the observation that at all levels "the intelligence objective should not be to remove the man from the loop, but to streamline organizations and communications to ensure that the right man is in the loop at the right moment."[37] While streamlining is perhaps driven more by the current downsizing and budget constraints, getting the right person in the loop still entails education and training along the lines of that previously discussed for information warriors. Here, too, in the intelligence community there will be a continuing effort to balance the use of AI systems which reduce the risk of information overload with the need to keep the man in the loop. But the trend toward evermore demanding education and training regimens for information warriors applies to NCOs as well as officers and poses some serious difficulties for recruiting and the Reserves in the Army.

The Education Dilemma

Wardynski has noted that the Army is now faced with the prospect of an enlisted force consisting mostly of college graduates much as it was faced with having to require its recruits to have high school diplomas in the late 1970s. He indicates that

> Information warfare implies multifaceted soldier skills as opposed to well-defined job tasks. Consequently, post-induction training many require months or years rather than weeks or months. Similarly, demands placed on soldiers, staffs and leaders are likely to grow in breadth, depth and complexity. This situation will further stretch the capabilities of reservists. Indeed, it is quite likely that the Reserves will find it increasingly difficult to acquire and maintain an acceptable level of capability.[38]

While conceding that the military will be in direct competition with industry in recruiting from the pool of college graduates, Wardynski offers no solid plan for attracting the suggested large numbers of them required to fill the ranks of information warriors. He does in passing suggest the possibility of "adapting information technology to a work force composed largely of high school graduates" but dispenses with that approach as not being cost effective and running counter to the industry trend to rely more and more on better educated individuals.[39] Clearly, there is a growing consensus that the military of tomorrow will have to fill its ranks with college graduates and continue to further educate and train them for extended periods after recruitment. Wardynski plays down the ability of technology to compensate for employing less highly educated individuals as information warriors. However, the use of AI systems would seem to be inevitable given the near real-time requirements of information-based warfare and information warfare.

Cybernetics Revisited

We are told that tomorrow's battlefield will be Cyberspace which has been loosely defined as "that consensually imagined universe where information reigns supreme. . .[consisting of] computers, modems, printers, fibers and wires of all sorts, antennas, electricity, intelligence, and the personnel who support these components."[40] Use of such terms as "Cyberspace" and "Cyberwar" harkens back to the heyday of cybernetics in the late 1950s and early 1960s. Ashby notes "cybernetics was defined by Wiener as 'the science of control and communication, in the animal and the machine'--in a word, as the art of steermanship. . ." Scientists in the Soviet Union were also pursuing research in this area, and an interesting comment on their efforts appeared in the Soviet press.

> In ancient Greece the man who steered ships was called Kybernetes. This steersman, whose name is given to one of the boldest sciences of the present--cybernetics--lives on in our time. He steers the space ships and governs the atomic installations, he takes part in working out the most complicated projects...[41]

Soviet scientists did not believe that cybernetics was a revolutionary new study. Rather, they saw it as a logical consequence of "the introduction of digital computing machines, automated assembly lines, automated factories, and the rapid development of automated industries."[42]

In the United States an engineer named Claude E. Shannon, who is well known by those working in communications, developed a particular branch of cybernetics that became what is now called information theory.[43] Now, as we move into the era of Third Wave warfare or information warfare, there is an evolving symbiotic relationship between man and the information systems he has created. The HMI is taking on characteristics that enable the human element to interchangeably share the duties of the steersman with the machine. This is a necessary and critical part of successfully waging information warfare, yet one that makes increasing demands on the human side of the HMI. Soviet, and now Russian, authors have written extensively on this important aspect of information warfare.

The Russian journal Military Thought in its first issue of 1995 included an article that provides considerable insight into how our former adversaries see

AI systems supporting decision makers. After detailing a number of complex problems associated with the proper functioning of Integrated Reconnaissance and Strike Systems (IRSS), the authors recommended solution is to utilize a hierarchy of intellectual systems for command and control which they define as "systems simulating human activity at the highest peak of human abilities (methodical, information, operational) and designed to fulfill practical missions that are called intellectual if performed by humans."[44] This proposal is certainly an outgrowth of the long-term emphasis on cybernetics in Russian R&D efforts. A distinction is made between the use of automation and 'intellectualization' which reflects the incorporation of higher-order human thought processes in what is called Intellectual Command and Control Systems (ICCS). The authors note such an approach is the only way to make decisions in real time for command and control of weapons systems and troops. Based on this article, it would seem that the Russians are more fully committed to using AI systems in conducting information warfare than we are. This would be expected based, as noted above, on their continued endeavors in cybernetics.

Reliance on Decision Support Systems (DSS)

In this country considerable progress has been made in developing and leveraging those technologies that can enhance expert systems and decision support systems for use in military operations. Of particular interest here is the ongoing work at the Battle Command Battle Lab (BCBL) at Fort Leavenworth, Kansas.

> The Battle Command Battle Lab (BCBL). . . is studying the impact of emerging information technology on weapon systems, C2, communications, intelligence and information systems. BCBL is also exploring ways to improve the commander's situational awareness, leading to more effective control of operational tempo through information technology.[45]

The ongoing efforts at BCBL are directed toward development of a DSS to be used by decision makers primarily at the tactical level of war. Their DSS will be tailored for use by Army commanders from the division down to the battalion. Known as a command support system (ComSS) the planned prototype will include a number of state-of-the-art capabilities such as automatic text and information-filtering services, artificial intelligence (AI), neural networks, and knowledge-based expert systems. Such 'cutting-edge' technology will nevertheless represent a significant challenge to those engineering this next generation of DSS for military use. The careful integration of information management is critical to avoiding information overload as noted earlier. The team at BCBL recognizes that the information flow will of necessity involve "numerous sources sending vast amounts of information across multiple communication channels..."[46] The authors do not address the additional training and education that will be required for effective use of the ComSS. However, they do note the possibility that "a seamless, jointly interoperable C2 system [the ComSS] may offset, to some degree, the combat capability lost as our military force structure is downsized, making the remaining forces more effective through improved C2. This overlooks, of course, the need for the very specialized talents of information warriors who would no doubt be required to effectively operate the ComSS.

Joint Doctrine and the People Side of Information Warfare

Joint Pub 1 describes the most important characteristics of modern warfare. These characteristics are related to (1) people, (2) technology, (3) the speed of communications and pace of events, (4) environment, and (5) friction, chance, and uncertainty.[47] This list is in a different order than that used by Joint Pub 1 with people first and environment fourth--the places of the others remain unchanged. The order here is one of priority or emphasis. After all, people are "the most important and constant element in warfare."[48] Without question, the United States has the most highly educated and best trained military in the world. In the past, leveraging of new technology on the battlefield has quite consistently given us a decided edge over our opponents by way of numerous force enhancements and force multipliers. But technology has also been the source of many problems. Modern technology is responsible for the increased speed of communications and pace of events as well as the wide range of lethal weapons now readily available to terrorists, drug traffickers, and rogue states. On the other hand, technology has to a great extent permitted our military forces to conquer land, sea, and air while taking a commanding lead in utilizing the space environment. It has also markedly reduced friction, chance, and uncertainty.

Clearly, technology is the underpinning of the current revolution in military affairs which encompasses information warfare. Joint Pub 1 notes

> ...the rapid evolution of technology in the postindustrial era (with its dramatic advances in information processing, advanced materials, robotics, and precision munitions) has altered warfare. Forces on land, at sea, and in the air now reinforce and complement each other more than ever before: in range of lethal striking power, common logistic and communications capabilities, and many other areas. Overhead, space-based capabilities affect all terrestrial forces, with a potential we have only begun to grasp.[49]

Actually, some visionaries have already grasped the potential of our expanding space-based capabilities recognizing that they are pivotal to the ability to conduct information warfare. Global presence, or what the Air Force has called virtual presence, would not be possible without the multitude of existing and planned space-based platforms. The Air Force's white paper on global presence submitted in late February 1995 precipitated a heated debate amongst the services on roles and missions as it appeared to play down the need for physical presence in favor of virtual presence. Further clarification was necessary to emphasize that virtual presence was not being offered as a substitute for physical presence but rather as one possible option in a complete range or spectrum of alternatives. The Air Force's director of plans noted that

> If we don't see the relationship between both ends of the spectrum [from physically engaged forces to nonphysical, informational forms of presence], we won't always have appropriate courses of action within our declining defense resources.[50]

The interaction between people and technology is complex but certainly determines whether and how well we see, develop, and adapt to new capabilities for military applications. Nowhere is this more apparent than in the current efforts to transition to information warfare as the preeminent mode of waging future conflicts. Arguably, the real center of gravity is not information but rather the information warriors themselves and the tools they must use including the omnipresent expert systems, intelligent systems and DSS.

People will make the critical difference. They always have. The challenge will be, as it has always been, to ensure that we have enough talented individuals to get the job done. Information warriors will be an elite group. The information warrior will be the operational commander's 'Cybernetes' to steer the proper course in the battlespace of the future.

NOTES

1. U.S. Joint Chiefs of Staff, National Military Strategy (Washington: February 1995), 15. Reference is also made here to the training necessary to ensure the lessons of Desert Storm can be taken full advantage of. This is important to the main issue investigated in the paper--the requirement for highly qualified people to become information warriors. Note the statement on page 18 which indicates "there is no substitute for high quality men and women in our Armed Forces."

2. U.S. Joint Chiefs of Staff, C4I for the Warrior (Washington: 12 June 1994), 9.

3. Ibid., 18.

4. U.S. Air Force Dept., Cornerstones of Information Warfare (Washington: 1995), 2.

5. Ibid. Note that the term 'information warfare' is used by most writers as a very general reference to all those areas included under command and control warfare (C2W) as well as the possible attacks which are now popularly referred to as Cyberwar or Netwar. Therefore, information warfare in most cases will implicitly include what the Air Force calls information age warfare.

6. William J. Perry, quoted in M. Robert Dresp, "Military Communications," IEEE Communications Magazine, October 1995, 84. The author notes the continuing efforts of the military to obtain "near perfect real-time knowledge of the enemy and communicate that to all forces in near real time."

7. U.S. Joint Chiefs of Staff, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations, Joint Pub 6-0 (Washington: 10 January 1995), I-4.

8. Julie Ryan and Gary Federici, Offensive Information Warfare--A Concept Exploration, Center for Naval Analyses, CIM 361 (Alexandria, VA: ESL, July 1994), 1.

9. J. R. Ullman, Pattern Recognition Techniques (New York: Crane-Russak, 1973), p. 1. Mathematical techniques of pattern recognition are implemented in hardware and software and collectively provide what is called artificial intelligence. The early work in this area was theoretical, but recent advances in computers, particularly parallel processors, have permitted widespread implementation of various image processing algorithms that can dramatically reduce the amount of information passed to users by selectively filtering only that of interest.

10. J.C.R. Licklider, quoted in Stephen J. Andriole and Gerald W. Hopple, ed., Defense Applications of Artificial Intelligence (Lexington, MA: Lexington Books, 1988), p. 145. This book devotes an entire chapter to artificial intelligence in command and control. Licklider worked for ARPA and this quote is taken from his work on human-computer symbiosis which was published in

1960.

11. Thomas P. Moran, ibid. The text indicates that a special issue of ACM Computing Surveys was published in March of 1981 covering the subject of human-computer interactions. Dr. Moran was the editor of that special issue of ACM Computing Surveys and the quote is taken from his editorial comments to that issue. The author indicates "Dr. Moran argued that we should improve the utility of computers by developing systems to expand the intellectual capability of the user and that to do so we need the attitudes of cognitive psychologists, not of engineers." The search for better ways to design systems of humans and machines has continued, but HMI problems in the past were often left for the users to solve.

12. Thomas Maguire, "Air Force Plans Net to Survive Nuclear Attack," Electronics, 22 March 1963, 28. The NMCS was the forerunner of the World-Wide Military Command and Control System (WWMCCS) which is now being replaced by the Global Command and Control System (GCCS).

13. "A Blast-Resistant Communications Network," Bell Laboratories Record, October 1965, 387.

14. U.S. Congrress, Senate, Committee on Armed Services, Recent False Alerts from the Nation's Missile Attack Warning System, Staff Report (Washington: U.S. Govt. Print. Off., 1980), 5-7.

15. Ibid., 8. The report also goes on to note that "the total system worked properly in that even though the mechanical electronic part produced erroneous information, the human part correctly evaluated it and prevented any irrevocable reaction."

16. Ibid., 8-9.

17. "Soviets Reject Explanation That Warning Alert Failed," Air Force Times, 23 June 1980, 3:2.

18. David Ansen, "High-Tech Paranoia," Newsweek, 30 May 1983, 99.

19. Robert Hatch, "Films - WarGames," The Nation, 23-30 July 1983, 92.

20. Jonathan Littman, "In the Mind of 'Most Wanted' Hacker, Kevin Mitnick," Computerworld, 15 January 1996, 87.

21. Ibid., 88. The author notes the very impressive talents of the notorious hacker Kevin Mitnick emphasizing the considerable time and experience that was necessary to develop and hone the skills which ended up getting him on the 'most wanted' list of the FBI. Indeed, based on Mitnick's story, there is an almost addictive quality to hacking that attracts certain individuals.

22. G.I. Wilson and Frank Bunkers, "Uncorking the Information Genie," Marine Corps Gazette, October 1995, 30.

23. Martin C. Libicki and James A. Hazlett, "Do We Need An Information Corps?" Joint Forces Quarterly, Autumn 1993, 97. While recognizing some of the pitfalls in creating a new organization, the authors cover many issues regarding the future of information warriors and why creation of an information corps makes good sense.

24. Ibid., 93. Short of a Ph.D. in Electrical Engineering and graduation from a senior service school coupled with many years of field experience, it's difficult to see how an individual would acquire the requisite skills to qualify as an information warrior based on these criteria.

25. Dean A. Nowowiejski, "Achieving Digital Destruction: Challenges for the M1A2 Task Force," Armor, January-February 1995, 24. The author notes the many challenges soldiers will face in exploiting the full capabilities of the M1A2 tank because of the advanced information systems it incorporates and the long learning curve required to operate them properly. In addition, he notes that "even though reports are quicker and more accurate in detail, they increase the volume of information and pick up the pace of operations, while continuing the requirement for interpretation." This, again, demonstrates the danger of information overload as we continue to compress the time frame for each OODA cycle.

26. Ibid.

27. Ibid.

28. Robert S. Walsh, "Information Enhancement on Today's Battlefield," Marine Corps Gazette, October 1995, 28.

29. Jeffrey B. Jones, "Theater Information Strategies," Military Review, November 1994, 50.

30. Ibid.

31. Morris J. Boyd and Michael Woodgerd, "Force XXI Operations," Military Review, November 1994, 20.

32. Ibid., 27.

33. James C. Madigan and George E. Dodge, "Battle Command: A Force XXI Imperative," Military Review, November 1994, 35.

34. Edward A. Smith, "Putting It Through the Right Window," U.S. Naval Institute Proceedings, June 1995, 38.

35. Ibid., 40.

36. Ibid.

37. Ibid.

38. E. Casey Wardynski, "The Labor Economics of Information Warfare," *Military Review*, May-June 1995, 60.

39. Ibid., 61.

40. Julie Ryan and Gary Federici, *Offensive Information Warfare--A Concept Exploration*, CIM 361, Center for Naval Analyses (Alexandria, VA: ESL, July 1994), 3.

41. Willis H. Ware and Wade B. Holland, ed., *Soviet Cybernetics Technology: I. Soviet Cybernetics, 1959-1962*, RM-3675-PR (Santa Monica, CA: Rand, June 1963), 10.

42. Ibid., 2.

43. "Cybernetics," *The New Encyclopedia Britannica, Micropedia*, 15th ed., v. 3, 818.

44. V.A. Denisenko and others, "Intellectual Command and Control Systems of Integrated Reconnaissance and Strike Systems of the Ground Forces," *Military Thought*, 1 January - February 1995, 55.

45. Michael L. McGinnis and George F. Stone III, "Decision Support Technology, *Military Review*, November 1994, p. 72.

46. Ibid., p. 74.

47. U.S. Joint Chiefs of Staff, *Joint Warfare of the Armed Forces of the United States*, Joint Pub 1 (Washington: 10 January 1995), I-1 - I-3.

48. Ibid. I-2.

49. Ibid.

50. Glenn W. Goodman, Jr., "The Power of Information," *Armed Forces Journal International*, July 1995, 24.

BIBLIOGRAPHY

Andriole, Stephen J. and Gerald W. Hopple, ed. Defense Applications of Artificial Intelligence. Lexington, MA: D.C. Heath and Company, 1988.

Ansen, David. "High-Tech Paranoia." Newsweek, 30 May 1983, 74.

Ashby, W. Ross. An Introduction to Cybernetics. New York: John Wiley & Sons, Inc., 1963.

Boyd, Morris J. and Michael Woodgerd. "Force XXI Operations." Military Review, November 1994, 17 - 28.

Campen, Alan D. "Rush to Information-Based Warfare Gambles with National Security." Signal, July 1995, 67 - 69.

"Cybernetics." The New Encyclopedia Britannica, Micropedia. 15th ed., v. 3, 818.

Denisenko, V. A., Ye. I. Suvorin, and P. S. Romanov. "Intellectual Command and Control Systems of Integrated Reconnaissance and Strike Systems of the Ground Forces." Military Thought, 1 January-February 1995, 54 - 59.

Dresp, M. Robert. "Military Communications." IEEE Communications Magazine, October 1995, 84 - 85.

Evanowsky, John B. "Information for the Warrior." IEEE Communications Magazine, October 1995, 106 - 112.

Goodman, Glenn W., Jr. "The Power of Information." Armed Forces Journal International, July 1995, 24.

Hatch, Robert. "Films-War Games." The Nation, 23 - 30 July 1983, 91 - 92.

Jones, Jeffrey B. "Theater Information Strategies." Military Review, November 1994, 48 - 50.

"Leveraging the Infosphere." Airpower Journal, Summer 1995, 8 - 25.

Libicki, Martin C. and James A. Hazlett. "Do We Need An Information Corps?" Joint Forces Quarterly, Autumn 1993, 88 - 97.

Littman, Jonathan. "In the Mind of 'Most Wanted' Hacker, Kevin Mitnick." Computerworld, 15 January 1996, 87 - 89.

Madigan, James C. and George E. Dodge. "Battle Command: A Force XXI Imperative." Military Review, November 1994, 29 - 39.

McGinnis, Michael L. and George F. Stone. "Decision Support Technology." Military Review, November 1994, 68 - 75.

Nowowiejski, Dean A. "Achieving Digital Destruction: Challenges for the M1A2 Task Force." Armor, January - February 1995, 21 - 24.

Pavlidis, T. Automatic Pattern Recognition. New York: Springer-Verlag, 1980.

Ryan, Julie and Gary Federici. Offensive Information Warfare--A Concept Exploration. CIM 361. Center for Naval Analyses. Alexandria, VA: ESL, July 1994.

Schickel, Richard. "Bigger Bangs for the Bucks." Time, 30 May 1983, 74.

Smith, Edward A., Jr. "Putting It Through the Right Window." U. S. Naval Institute Proceedings, June 1995, 38 - 40.

"Soviets Reject Explanation That Warning Alert Failed." Air Force Times, 23 June 1980, 3:2.

U. S. Air Force Dept. Cornerstones of Information Warfare. Washington: 1995.

U. S. Congress. Senate. Committee on Armed Services. Recent False Alerts from the Nation's Missile Attack Warning System. Staff Report. Washington: U. S. Govt. Print. Off., 1980.

U. S. Joint Chiefs of Staff. C4I for the Warrior. Washington: 12 June 1994.

U. S. Joint Chiefs of Staff. Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. Joint Pub 6-0. Washington: 30 May 1995.

U. S. Joint Chiefs of Staff. Joint Warfare of the Armed Forces of the United States. Joint Pub 1. Washington: 10 January 1995.

U. S. Joint Chiefs of Staff. National Military Strategy. Washington: February 1995.

Walsh, Edward J. "The Copernican Revolution." Armed Forces Journal International, July 1995, 40 - 42.

Walsh, Robert S. "Information Enhancement on Today's Battlefield." Marine Corps Gazette, October 1995, 27 - 29.

Wardynski, E. Casey. "The Labor Economics of Information Warfare." *Military Review*, May - June 1995, 56 - 61.

Ware, Willis H. and Wade B. Holland, ed. *Soviet Cybernetics Technology: I. Soviet Cybernetics, 1959 - 1962*. RM-3675-PR. Santa Monica, CA: Rand, June 1963.

Wilson, G. I. and Frank Bunkers. "Uncorking the Information Genie." *Marine Corps Gazatte*, October 1995, 29 - 31.